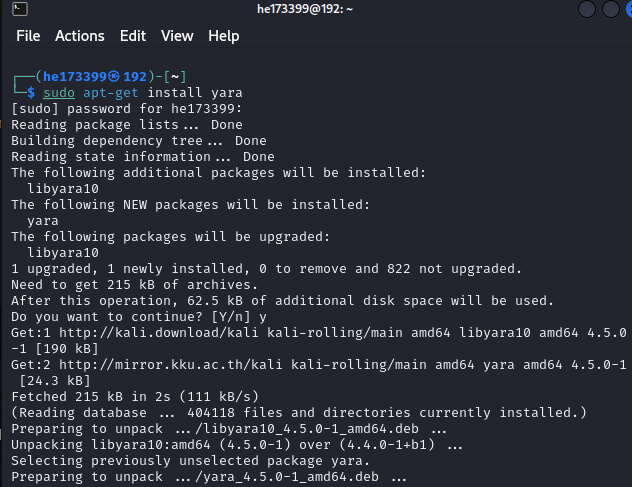
LAB 4: Detect Malware Capabilities with YARA

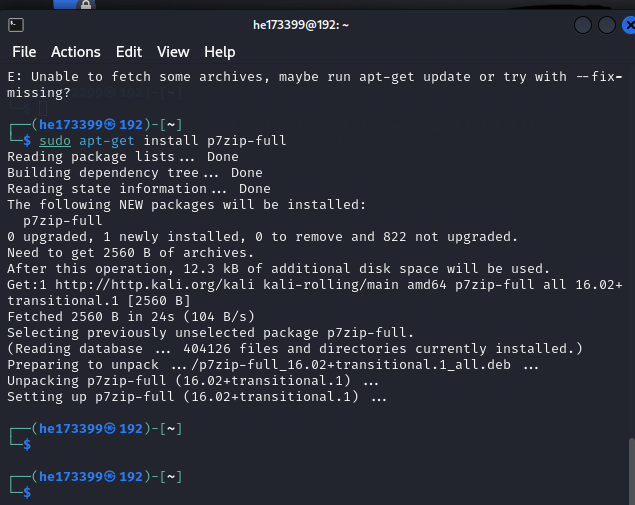
- YARA is a popular tool that provides a robust language.

- It is used to examine the suspected files/directories and match strings as is defined in the YARA rules with the file. Install YARA

sudo apt-get install yara 

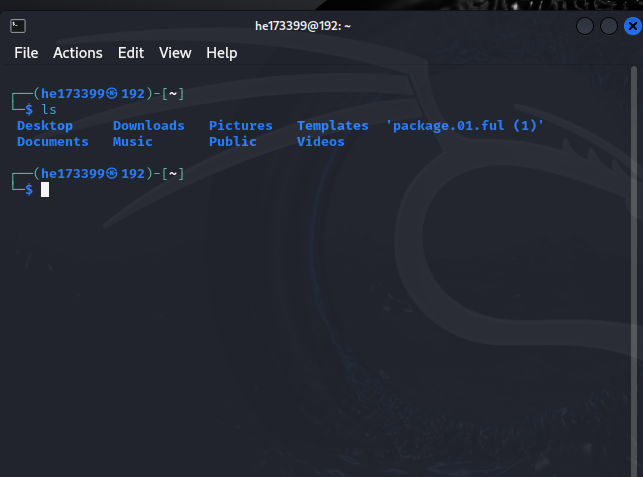
Download package.01.ful.7z:

sudo apt-get install p7zip-full

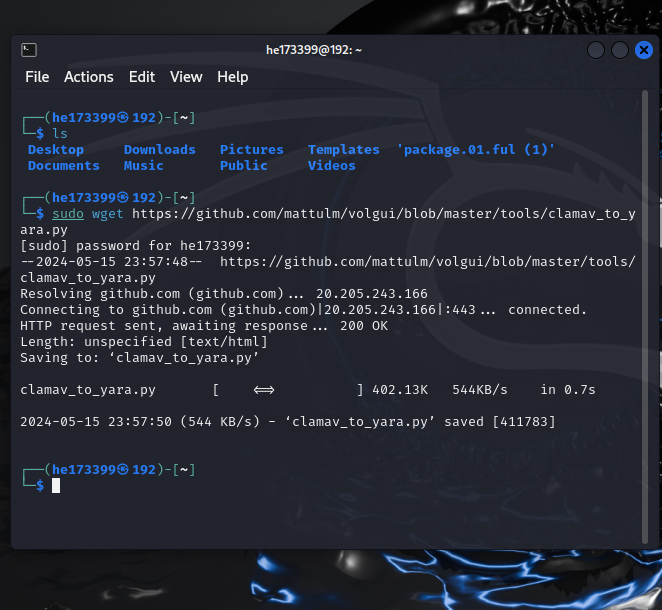


<https://code.google.com/archive/p/clamsrch/downloads>

ls

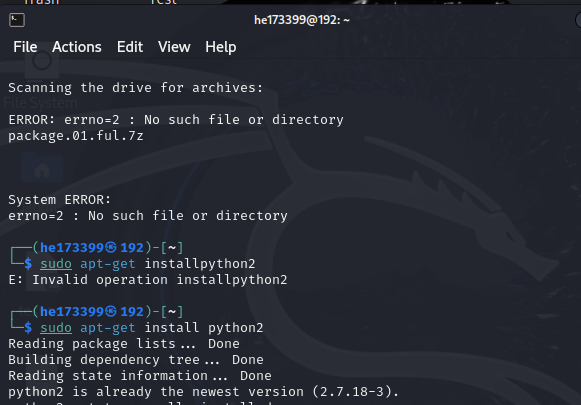


sudo wget <https://github.com/mattulm/volgui/blob/master/tools/clamav_to_yara.py>

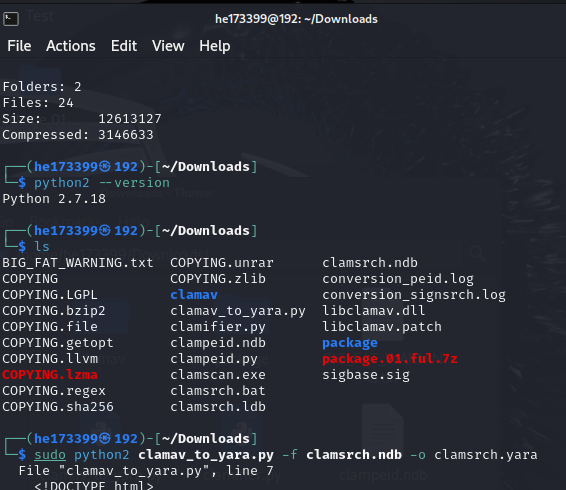


install python2

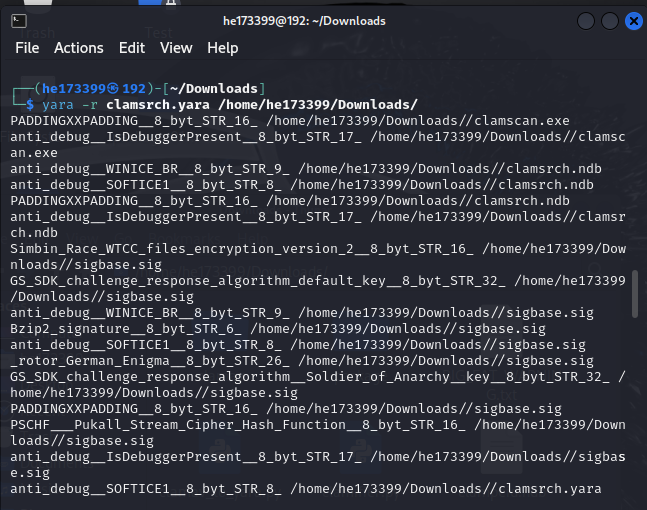
sudo apt-get install python2



sudo python2 clamav\_to\_yara.py -f clamsrch.ndb -o clamsrch.yara

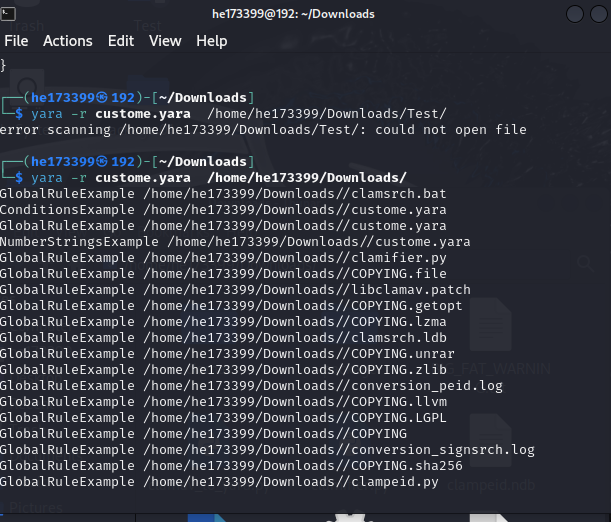


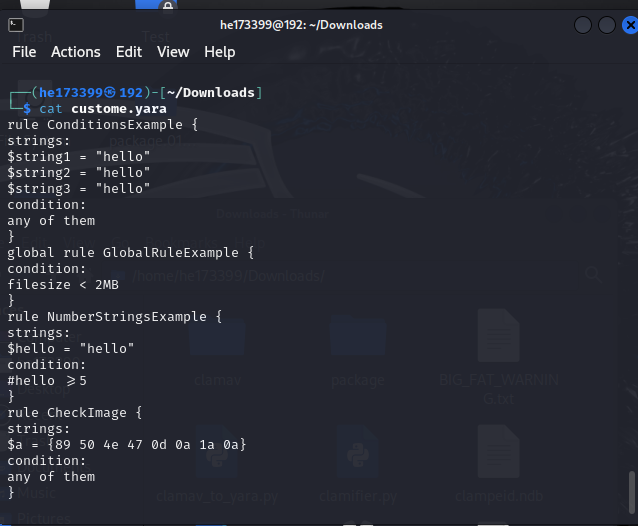
yara -r clamsrch.yara /home/he173399/Downloads/



Test yara rules:

yara -r custome.yara /home/he173399/Downloads/



Create a new rule file called custome.yara

Test yara rules:

